CLAIMS

1. A method for a security manager device to manage a plurality of network security devices with a plurality of supervisor devices, each network security device generating network security information related to an associated group of network devices, storing the generated network security information on a primary supervisor device for the network security device when the primary supervisor device is available to store the generated network security information, and storing the generated network security information on an alternate supervisor device when the primary supervisor device is unavailable, the method comprising:

distributing security control information to multiple network security devices, the security control information to be used to generate network security information, by

determining a supervisor device that is the primary supervisor device for each of the multiple network security devices;

sending a single copy of the security control information to the determined supervisor device; and

indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices; and

aggregating the network security information generated by an indicated one of the multiple network security devices using the security control information, by

determining at least one alternate supervisor device that stores at least a portion of the network security information generated by the indicated network security device;

notifying the primary supervisor device for the indicated network security device of a desire for the generated network security information, the notifying including an indication of the determined alternate supervisor devices; and

in response, receiving the generated network security information,

so that the manager device can efficiently distribute information to multiple network security devices, and can retrieve all of the generated network security information for a network security

device because alternate supervisor devices will store the information when the primary supervisor device for the network security device is unavailable.

2. The method of claim 1 including generating network security information by, for each network security device:

monitoring network information passing between any network device in the associated group for the network security device and any network device not in the associated group; and

when the monitored network information is of an indicated type,

determining whether the primary supervisor device for the network security device is available to receive information;

when the primary supervisor device is available, sending network security information about the monitored network information to the primary supervisor device for storage; and

when the primary supervisor device is not available, sending network security information about the monitored network information to an alternate supervisor device for storage.

3. The method of claim 2 wherein for each network security device, a security policy for the network security device specifies the indicated types of monitored network information for which to generate network security information and specifies data related to the monitored network information to be included in the generated network security information.

4. The method of claim 1 wherein the distributed security control information is software to be executed by the multiple network security devices to control the generation of the network security information.

5. The method of claim 1 wherein the distributed security control information is a security policy template that defines the network security information to be generated, and including:

after a copy of the security policy template has been sent to each of the multiple network security devices, configuring each copy of the security policy template with information specific to the network security device to which the security policy template was sent.

6. The method of claim 1 wherein after the notifying of the primary supervisor device, the primary supervisor device sends the generated network security information to the manager device by:

retrieving from each of the determined alternate supervisor devices the network security information generated by the indicated network security device;

retrieving any network security information generated by the indicated network security device that is stored by the primary supervisor device; and

sending the retrieved network security information to the manager device.

7. The method of claim 1 including after the receiving of the generated network security information, aggregating the portions of the generated network security information stored by the determined alternate supervisor devices and any portion of the generated network security information stored by the primary supervisor device.

8. The method of claim 1 wherein information is sent between the manager device and the supervisor devices and between the supervisor devices and the network security devices in a secure form so that others do not have access to contents of the information.

9. The method of claim 1 including displaying to a user the plurality of network security devices and the plurality of supervisor devices in such a manner that the primary supervisor device for each of the network security devices is visually indicated, and wherein the distributing of the security control information to the multiple network security devices is in response to selection by the user of the displayed multiple network security devices.

10. The method of claim 1 including displaying to a user the plurality of network security devices and the plurality of supervisor devices in such a manner that the primary supervisor device for each of the network security devices is visually indicated, and wherein the aggregating of the network security information generated by an indicated one of the multiple network security devices is in response to a visual indication by the user of the one multiple network security device.

11. A method for collecting security information generated by a security device, the generated security information based on network information passing between other network devices, the generated security information stored on at least one host device distinct from the security device, the method comprising:

receiving a request for the generated security information;

determining the host devices on which at least portions of the generated security information are stored; and

when there are multiple determined host devices,

for each of the multiple determined host devices, retrieving the portions of the generated security information that are stored on the host device; and

aggregating the retrieved portions of the generated security information.

12. The method of claim 11 including determining a host device that is a primary host device for the security device, and wherein the portions of the generated security information from each of the multiple determined host devices are retrieved from the primary host device after the primary host device collects the portions from the multiple determined host devices.

13. The method of claim 11 including requesting from each of the multiple determined host devices the portions of the generated security information that are stored on the host device.

14. The method of claim 11 wherein the aggregating of the retrieved portions of the generated security information includes sorting the aggregated security information chronologically.

15. The method of claim 11 wherein the aggregating of the retrieved portions of the generated security information includes sorting the aggregated security information by type of security information.

16. The method of claim 11 wherein the received request for the generated security information is from a user, and including displaying the aggregated security information to the user.

17. The method of claim 11 including determining a change needed in network information allowed to pass between the other network devices based on the aggregated security information.

18. The method of claim 11 including displaying to a user a view including the security device and the host devices, and wherein the request for the generated security information involves a visual indication by the user of the security device.

19. A method for collecting security information generated by a security device, the generated security information based on network information passing between other network devices, the generated security information stored on multiple host devices distinct from the security device, the method comprising:

receiving a request from a manager device for the generated security information;

receiving an indication of the multiple host devices which store portions of the generated security information;

retrieving from each of the multiple host devices the stored portions of the generated security information; and

sending to the manager device the retrieved portions of the generated security information,

so that the manager device can aggregate the portions of the generated security information stored by the multiple host devices.

20. The method of claim 19 including:

before sending to the manager device the retrieved portions of the generated security information, determining that the manager device is predefined as being authorized to receive the generated security information.

21. The method of claim 19 including:

receiving from the manager device access information; and

before sending to the manager device the retrieved portions of the generated security information, determining that the access information authorizes a sender of the access information to receive the generated security information.

22. The method of claim 19 including:

before sending to the manager device the retrieved portions of the generated security information, formatting the retrieved portions in a manner accessible only to the manager device.

23. The method of claim 19 wherein the indications of the multiple host devices which store portions of the generated security information is received from the manager device.

24. The method of claim 19 including before receiving the indications of the multiple host devices which store portions of the generated security information, contacting the security device to determine the multiple host devices.

25. A method for storing security information generated by a security device in a distributed manner so as to ensure the security information is available, the security information based on network information passing between network devices, the method comprising:

identifying whether a primary supervisor device for the security device is available to store received security information;

when the primary supervisor device is available, storing the security information on the primary supervisor device; and

when the primary supervisor device is not available, storing the security information on an alternate supervisor device,

so that a manager device can retrieve all of the security information because alternate supervisor devices will store the information when the primary supervisor device is unavailable.

26. The method of claim 25 including generating the security information by:

retrieving a policy which indicates types of network information;

monitoring the network information passing between the network devices; and

when the monitored network information is of a type indicated by the policy, generating security information about the monitored network information.

27. The method of claim 26 wherein the policy for the network security device indicates types of information to be included in the generated security information.

28. The method of claim 25 including:

before storing the security information on a supervisor device, determining that the supervisor device is predefined as being authorized to receive the security information.

29. The method of claim 25 including:

before storing the security information on a supervisor device, formatting the security information in a manner accessible only to the supervisor device.

30. The method of claim 25 wherein the method is performed by the security device, and including sending the security information to the supervisor device that will store the security information in a manner accessible only to the supervisor device.

31. A method for distributing security policy implementation information to multiple security devices for use in implementing a security policy, the method comprising:

for each of the security devices, determining a supervisor device currently associated with the security device;

distributing the security policy implementation information to each of the determined supervisor devices; and

indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated.

32. The method of claim 31 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

33. The method of claim 31 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

34. The method of claim 33 including:

after the security policy implementation information has been distributed to each of the security devices, configuring the security policy implementation information distinctly on each security device.

35. The method of claim 31 wherein the security policy implementation information is an instruction to be executed by the multiple security devices related to the implementing of the security policy.

36. The method of claim 31 wherein the security policy implementation information is information common to the multiple security devices, and wherein for each of the multiple security devices the common information is for configuring a security policy template for the security device with information specific to the security device.

37. The method of claim 31 wherein before the security policy implementation information is distributed to each of the multiple security devices, at least some of the multiple security devices have existing security policy implementation information of a similar type, and wherein for those security devices the security policy implementation information to be distributed will replace the existing security policy implementation information.

38. The method of claim 31 wherein before the security policy implementation information is distributed to each of the multiple security devices, at least some of the multiple security devices have existing security policy implementation information of a similar type, and wherein for those security devices the security policy implementation

information to be distributed will supplement the existing security policy implementation information.

39. The method of claim 31 wherein the distributing of the security policy implementation information to each of the determined supervisor devices is performed in a manner such that the security policy implementation information is not accessible to other devices.

40. The method of claim 31 including displaying to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and wherein the distributing of the security policy implementation information is in response to a visual selection by the user.

41. A method for a supervisor device to distribute security policy implementation information to multiple security devices for use in implementing a security policy, the method comprising:

receiving from a manager device a single copy of security policy implementation information to be distributed to multiple security devices; and

for each of the multiple security devices, if the supervisor device is associated with the security device, distributing the security policy implementation information to the security device.

42. The method of claim 41 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

43. The method of claim 41 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

44. The method of claim 43 including:

after the security policy implementation information has been distributed to each of the security devices, configuring the security policy implementation information distinctly on each security device.

45. The method of claim 43 including:

before the security policy implementation information has been distributed to each of the security devices, for each security device configuring distinctly for that device a copy of the security policy implementation information that is to be distributed to that device.

46. The method of claim 43 including:

for each of the security devices, sending to the security device a control instruction indicating an action to be taken with the security policy implementation information by the security device.

47. The method of claim 41 wherein the security policy implementation information is an instruction to be performed by the security devices related to the implementing of the security policy.

48. The method of claim 41 wherein the supervisor device distributes the security policy implementation information to a security device only when the supervisor device is associated with the security device as a primary supervisor device for the security device.

49. The method of claim 41 including when the supervisor device is not associated with one of the multiple security devices, distributing the security policy implementation information to another supervisor device to be distributed to the one security device.

50. A method for distributing control information to multiple security devices for use in controlling the operation of the multiple security devices, the method comprising:

for each of the security devices, determining a supervisor device currently associated with the security device;

distributing the control information to each of the determined supervisor devices; and

indicating to each of the determined supervisor devices to distribute the control information to the security devices with which the supervisor device is associated.

51. The method of claim 50 wherein after the control information is distributed to the security devices, the security devices operate in accordance with the control information.

52. A method for a security device to operate in accordance with security policy implementation information distributed from a manager device, the method comprising:

receiving security policy implementation information to be used by the security device in implementing a security policy; and

using the security policy implementation information to implement the security policy.

53. The method of claim 52 wherein the security policy implementation information is distributed to multiple security devices via a supervisor device associated with the multiple security devices.

54. The method of claim 52 wherein the security policy implementation information is software to be executed by the security device to control the implementing of the security policy.

55. The method of claim 52 wherein the security policy implementation information is a security policy template that indicates security information to be generated.

56. The method of claim 55 including:

after the security policy implementation information has been received, receiving from the manager device configuration information specific to the security device to customize the security policy template.

57. The method of claim 52 wherein the security policy implementation information is an instruction to be taken by the security device related to the implementing of the security policy.

58. The method of claim 52 including:

before using the security policy implementation information to implement the security policy, determining that the manager device is predefined as being authorized to distribute the security policy implementation information.

59. The method of claim 52 including:

receiving from the manager device access information; and

before using the security policy implementation information to implement the security policy, determining that the access information authorizes a sender of the access information to distribute the security policy implementation information.

60. A method for collecting security information generated by a security device, the generated security information based on network information passing between other network devices, the generated security information stored on at least one host device distinct from the security device, the method comprising:

displaying to a user a view including the security device and the host devices;

receiving from the user a visual indication of a security device from which to retrieve generated security information;

determining the host devices on which at least portions of the generated security information are stored;

retrieving the portions of the generated security information that are stored on the determined host devices; and

aggregating the retrieved portions of the generated security information.

61. The method of claim 60 including displaying to the user the aggregated generated security information.

62. The method of claim 60 wherein the view of the security device and of the host devices includes a visual indication of a host device that is a primary host device for the security device.

63. The method of claim 60 wherein the view of the security device and of the host devices includes visual indications of the determined host devices.

64. The method of claim 60 wherein a visual indication displayed in the view of a device performing the method is modified to indicate that the generated security information has been retrieved.

65. A method for distributing security policy implementation information to multiple security devices for use in implementing a security policy, the method comprising:

displaying to a user a view of the multiple security devices and of multiple supervisor devices;

receiving from the user visual indications of multiple security devices to which the security policy implementation information is to be distributed;

distributing the security policy implementation information to a supervisor device associated with each of the security devices; and

indicating to the associated supervisor device to distribute the security policy implementation information to each of the security devices.

66. The method of claim 65 including:

displaying to the user multiple pieces of security policy implementation information; and

determining the security policy implementation information to be distributed based on a visual indication by the user.

67. The method of claim 65 wherein the view of the security devices and of the supervisor devices includes a visual indication of a supervisor device that is a primary host device for the security device.

68. The method of claim 65 wherein a visual indication for each of the multiple security devices is modified to indicate receipt by the security device of the security policy implementation information.

69. A method for displaying security information generated by a security device, the generated security information based on network information passing between other network devices, portions of the generated security information stored on multiple host devices distinct from the security device, the method comprising:

displaying to a user a view including the security device and the host devices;

receiving from the user an indication of a security device from which to retrieve generated security information; and

displaying to the user an aggregation of the portions of the generated security information retrieved from the multiple host devices.

70. The method of claim 69 wherein the view of the security device and of the host devices includes visual indications of the multiple host devices.

71. The method of claim 69 wherein a visual indication displayed in the view of a device performing the method is modified to indicate that the generated security information has been retrieved.

72. A method for distributing security policy implementation information to multiple security devices for use in implementing a security policy, the method comprising:

displaying to a user a view of a manager device, the multiple security devices and of multiple supervisor devices;

receiving from the user indications of multiple security devices to which the security policy implementation information is to be distributed; and

displaying to the user an indication that the security policy implementation information is distributed to the multiple security devices, the distribution accomplished by the manager device sending the security policy implementation information to a supervisor device associated with each of the security devices and indicating to the associated supervisor device to distribute the security policy implementation information to each of the security devices.

73. The method of claim 72 including:

displaying to the user multiple pieces of security policy implementation information; and

determining the security policy implementation information to be distributed based on a visual indication by the user.

74. The method of claim 72 wherein the view of the security devices and of the supervisor devices includes a visual indication that the associated supervisor device distributes the security policy implementation information to each of the security devices.

75. The method of claim 72 wherein a visual indication for each of the multiple security devices is modified to indicate receipt by the security device of the security policy implementation information.

76. The method of claim 72 wherein the multiple security devices to which the security policy implementation information is to be distributed are indicated from a selection by the user of the associated supervisor device.

77. A computer-readable medium whose contents cause a manager device to collect security information generated by a security device, the generated security information based on network information passing between other network devices, the generated security information stored on at least one host device distinct from the security device, by:

receiving a request for the generated security information;

determining the host devices on which at least portions of the generated security information are stored; and

when there are multiple determined host devices,

for each of the multiple determined host devices, retrieving the portions of the generated security information that are stored on the host device; and

aggregating the retrieved portions of the generated security information.

78. The computer-readable medium of claim 77 wherein the contents further cause the manager device to determine a host device that is a primary host device for the security device, and wherein the portions of the generated security information for each of the multiple determined host devices are retrieved from the primary host device.

79. The computer-readable medium of claim 77 wherein the aggregating of the retrieved portions of the generated security information includes sorting the aggregated security information chronologically.

80. The computer-readable medium of claim 77 wherein the received request for the generated security information is from a user, and wherein the contents further cause the manager device to display the aggregated security information to the user.

81. The computer-readable medium of claim 77 wherein the contents further cause the manager device to display to a user a view including the security device and the host devices, and wherein the request for the generated security information involves a visual indication by the user of the security device.

82. A computer-readable medium whose contents cause a manager device to distribute security policy implementation information to multiple security devices for use in implementing a security policy, by:

for each of the security devices, determining a supervisor device currently associated with the security device;

distributing the security policy implementation information to each of the determined supervisor devices; and

indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated.

83. The computer-readable medium of claim 82 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

84. The computer-readable medium of claim 82 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

85. The computer-readable medium of claim 84 wherein the contents further cause the manager device to, after the security policy implementation information has been distributed to each of the security devices, configure the security policy implementation information distinctly on each security device.

86. The computer-readable medium of claim 82 wherein the security policy implementation information is an instruction to be executed by the multiple security devices related to the implementing of the security policy.

87. The computer-readable medium of claim 82 wherein the contents further cause the manager device to display to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and wherein the distributing of the security policy implementation information is in response to a visual selection by the user.

88. A computer system for collecting security information generated by a security device, the generated security information based on network information passing between other network devices, the generated security information stored on at least one host device distinct from the security device, comprising:

a user interface component that receives from a user a request for the generated security information; and

a security information retriever that determines the host devices on which at least portions of the generated security information are stored, and that when there are multiple determined host devices, for each of the multiple determined host devices, retrieves the portions of the generated security information that are stored on the host device and aggregates the retrieved portions of the generated security information.

89. The computer system of claim 88 wherein the user interface component is capable of generating a graphical display of the aggregated security information.

90. The computer system of claim 88 wherein the user interface component is capable of generating a graphical display including a hierarchical view of the security device and the host devices, and wherein the user interface component is further for receiving a visual indication of the security device indicating the request for the generated security information of the indicated security device.

91. A computer system for distributing security policy implementation information to multiple security devices for use in implementing a security policy, comprising:

a security device associator for determining for each of the security devices a supervisor device currently associated with the security device; and

an information distributor for distributing the security policy implementation information to each of the determined supervisor devices, and for indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated.

92. The computer system of claim 91 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

93. The computer system of claim 91 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

94. The computer system of claim 91 including a user interface component for displaying to a user a view of the multiple security devices and the supervisor devices currently associated with the security devices, and for receiving a visual selection by the user that controls the distributing of the security policy implementation information.

95. A computer system for storing security information generated by a security device in a distributed manner so as to ensure the security information is available, the security information based on network information passing between network devices, comprising:

a storage identifier for identifying whether a primary supervisor device for the security device is available to store received security information; and

an information storer for storing the security information on the primary supervisor device if the primary supervisor device is available, and for storing the security information on an alternate supervisor device when the primary supervisor device is not available.

96. The computer system of claim 95 further comprising:

a security information generator for retrieving a policy which indicates types of network information, for monitoring the network information passing between the network devices, and for generating security information about the monitored network information when the monitored network information is of a type indicated by the policy.

97. The computer system of claim 95 further comprising:

a security component for determining that a supervisor device is predefined as being authorized to receive the security information before storing the security information on the supervisor device.

98. A computer system that implements a security policy in accordance with security policy implementation information distributed from a manager device, comprising:

a security policy information receiver for receiving security policy implementation information to be used in implementing a security policy; and

a security policy implementer for using the security policy implementation information to implement the security policy.

99. The computer system of claim 98 wherein the security policy implementation information is software to be executed by the security device to control the implementing of the security policy.

100. The computer system of claim 98 wherein the security policy implementation information is a security policy template that indicates security information to be generated.

101. The computer system of claim 98 further comprising:

a security component for determining that the manager device is predefined as being authorized to distribute the security policy implementation information before using the security policy implementation information to implement the security policy.

102. A generated data signal transmitted via a data transmission medium from a manager device to a supervisor device, the data signal including a single copy of security policy implementation information to be distributed by the supervisor device to multiple security devices, the security policy implementation information for use by the supervisor devices in implementing a security policy,
so that the manager device can efficiently distribute information to multiple security devices via a supervisor device.

103. The data signal of claim 102 wherein the security policy implementation information is software to be executed by the security devices to control the implementing of the security policy.

104. The data signal of claim 102 wherein the security policy implementation information is a security policy template that indicates the security information to be generated.

105. The data signal of claim 102 including configuration information to be distributed by the supervisor device to at least one security device, the configuration information specific to the at least one security device, the configuration information for configuring distinctly for the at least one security device a copy of the security policy implementation information that is to be distributed to that device.